Trustworthy Coordination of Web Services Atomic Transaction for Net Banking

Supriya Kurian* & Ramya. G. Franklin**

*Research Student, Department of Master of Computer Applications, Sathyabama University, Chennai, Tamilnadu, INDIA.
E-Mail: supriyakurian49@yahoo.com
**Assistant Professor, Department of Master of Computer Applications, Sathyabama University, Chennai, Tamilnadu, INDIA.
E-Mail: mikella.prabu@gmail.com

***Abstract*—**Nowadays, in net banking sector they use 2PC protocol. But, it is problematic for single site failures. We have used the formal model of distributed commit protocols in the process algebra mCRL2. We applied this method to the Three-Phase Commit protocol and proved that it is erroneous for simultaneous site failures. For the security of transaction SOAP protocol is used. In this, user will enter their user id, password and one-time password for accessing their account. They can view all their transactions across all branches of Net Bank locations online and do transactions within the bank network. By using this, it is possible to make the transaction more fast and can reduce interruption. It will also protect the WS-AT (Web Service-Atomic Transaction) services. Useful for business applications based on transactional Web Services that require a high degree of dependability, security and trust.

***Keywords*—**Atomic Transactions, Authentication, Byzantine Agreement, Encryption, Message Authentication Code, Security, Web Services

***Abbreviations*—**Application Programming Interfaces (API), Electronic Fund Transfer (EFT), Message Authentication Code (MAC), Online Transaction Processing (OLTP), Simple Object Access Protocol (SOAP),

I. INTRODUCTION

WEB services are Application Programming Interfaces (API) or Web APIs that are accessed via Hypertext Transfer Protocol (HTTP). It is a method of communication between two electronic devices over the World Wide Web [http://en.wikipedia.org/wiki/Web_service]. A Web service is a software function provided at a network address over the web. It has an interface described in a machine-processable format (specifically Web Services Description Language, known by the acronym WSDL). Other systems interact with the Web service in a manner prescribed by its description using SOAP messages. This system will reduce the interruption because of site failures. In this system, we used two protocols. SOAP protocol is used for the secure transaction and 3PC protocol for the simultaneous site failures [Gudgin et al., 2007]. In bank side, for the security of details of the client, Message Authentication Codes (MAC) algorithm is used. Also in the client side, while the client type his/her account number that time also the account number will be encrypted by using MAC algorithm. A MAC is a security code that is typed in by the user of a computer to access accounts or portals [http://www.investopedia.com/terms/m/message-authentication-code.asp]. This code is attached to the message or request sent by the user. MACs attached to the message must be recognized by the receiving system in order to grant the user access. MACs are commonly used in Electronic Funds Transfers (EFTs) to maintain information integrity. The test application is modified so that all messages exchanged within each transaction are protected by a message authentication code.

II. RELATED WORKS

The coordination of Web services has been previously addressed by Honglei Zhang et al., (2012) in the Trustworthy coordination of Web services atomic transaction by using 2PC protocol. It shows how to avoid naively applying a general-purpose BFT algorithm by exploiting the semantics of WS-AT operations to reduce the number of Byzantine agreements needed to achieve atomic termination of a Web Services Atomic Transaction. The PBFT has been discussed in Practical Byzantine Fault Tolerance [Castro & Liskov, 1999]. It says software bugs, operator mistakes, and malicious attacks are a major cause of service interruptions and they can cause arbitrary behavior, that is, Byzantine

faults. In the trustworthy coordination of web services atomic transaction for net banking we have described a suite of protocols and mechanisms that protect the WS-AT services and infrastructure against Byzantine faults. The main contribution of this paper is that it shows how to avoid naively applying a general-purpose BFT algorithm (i.e., totally ordering all incoming requests at the replicated Coordinator), by exploiting the semantics of WSAT operations to reduce the number of Byzantine agreements needed to achieve atomic termination of a Web Services Atomic Transaction.

III. COORDINATION OF WEB SERVICES

In the "Trustworthy Coordination of Web Services Atomic Transaction for Net Banking", we use the 3PC (Three Phase Commit) protocol [Pallemulle et al., 2008; Honglei Zhang et al., 2012]. 3PC prevents blocking situation in the absence of communications failures [http://en.wikipedia.org/wiki/Three-phase_commit_protocol]. It can be made resilient to communications failures, but then it may block. 3PC is actually more complex than 2PC protocol, but only marginally improves reliability, prevents some blocking situations. Because of this, 3PC is not used much in practice. The main idea is that becoming certain and deciding to commit are separate steps. 3PC ensures that if any operational process is uncertain, then no (failed or operational) process has committed. So, in the termination protocol, if the operational processes are all uncertain, they can decide to abort (avoids blocking).

3.1. Architecture of Proposed System

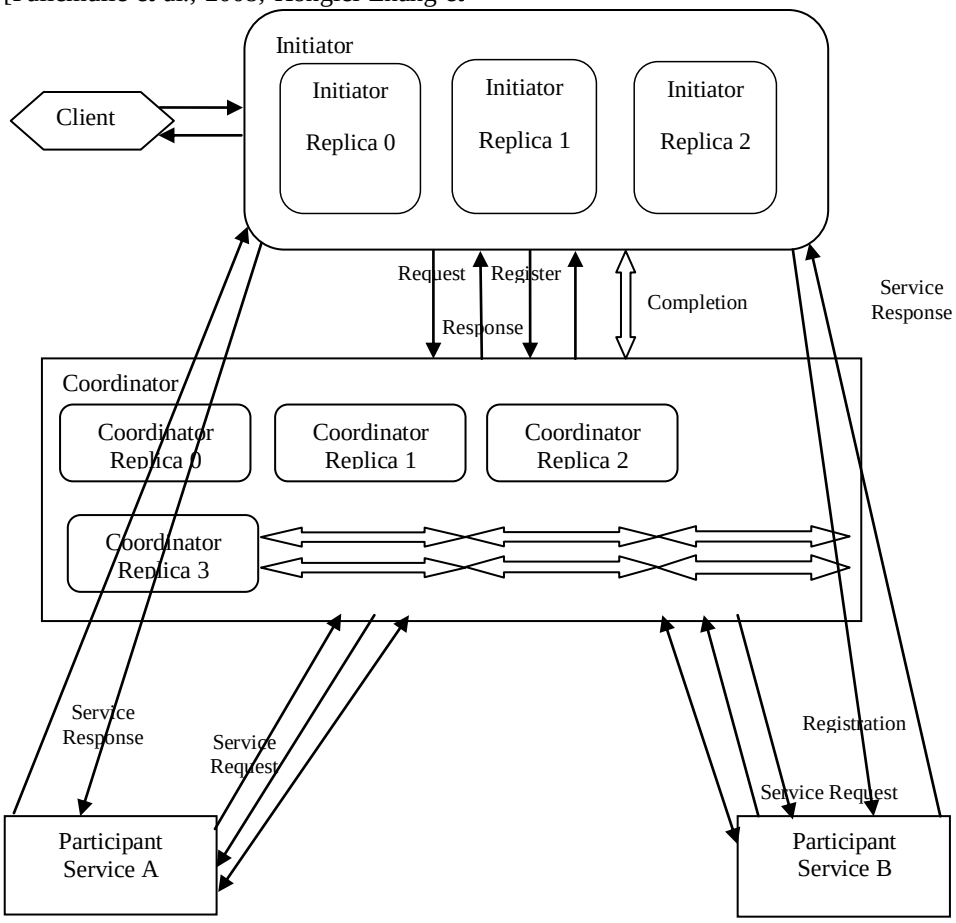


Figure 1 – Architecture Diagram

IV. EXPERIMENTAL RESULT

This system is based on Net Banking. In this, we show how to do transaction securely and without interruption. For the security we have used one-time password and SOAP protocol [Steiner et al., 1996]. When the authorized user types his username and password, one-time password will send to their email address [http://en.wikipedia.org/wiki/One-time_password]. Then he/she needs to type account number, card number and password. When the client enters his/her account number it will be encrypted by using MAC encryption algorithm. And the coordinator will decrypt it using MAC decryption algorithm to check whether it is an authorized user or not. If it is an authorized user then the coordinator will allow the user to do the transaction and if not, error message will display. After getting inside the account he can do further transactions. Here, SOAP protocol

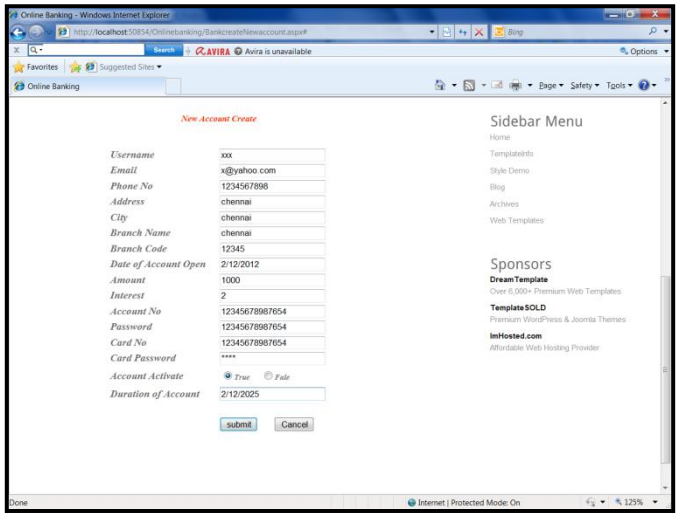
is used for securely transferring the transaction details. So, intruders cannot hack the details. For the interruption problems we used three replica Web services other than the main Web service. Here, 3PC protocol is used, by using Byzantine Agreement Algorithm it will check whether Web service is active or not. If the Web service is active, it will respond with acknowledgement and with that Web service we will do the transaction. And if inactive by using Byzantine Agreement Algorithm the coordinator will search for other replica services and which will respond as active the connection will switch to that service using 3PC protocol [Zhao, 2007; Zhao, 2007A; en.wikipedia.org/wiki/Quantum_Byzantine_agreement]. So that, the user can does the transactions without any interruption.

Bank can login with the particular username and password. It can create account for the user. While the account creation we used MAC Algorithm for encrypting the details of the user. Bank can also create IFSC code for each bank; view the user details and transaction also.

Coordinator can view all the user details and transactions across the banks. He will monitor all the banks activities. Coordination also has a username and password.

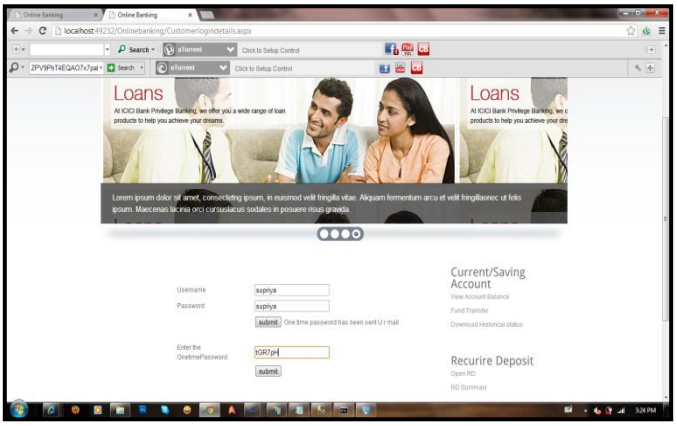
V. RESULTS AND DISCUSSION

New Account Creation



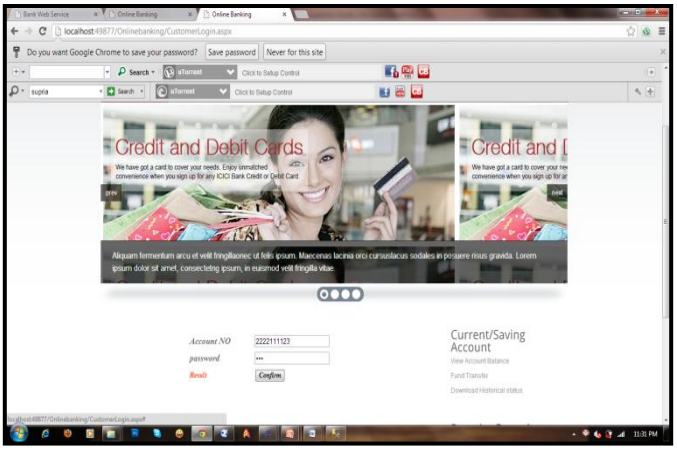
New customers give all the information to bank. Bankers analyze all the information of the customer. If all the information provided is correct then, allow to create the new account for the particular customer.

Customer Login



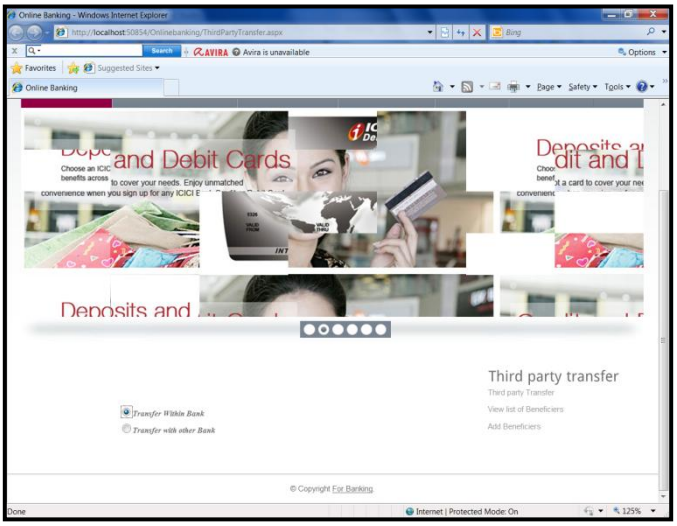
Allows authorized users to login using their username and password. Here the user needs to give their username and password. Then the coordinator will generate a one-time password to the users email. Using that password user can login.

Account Verification



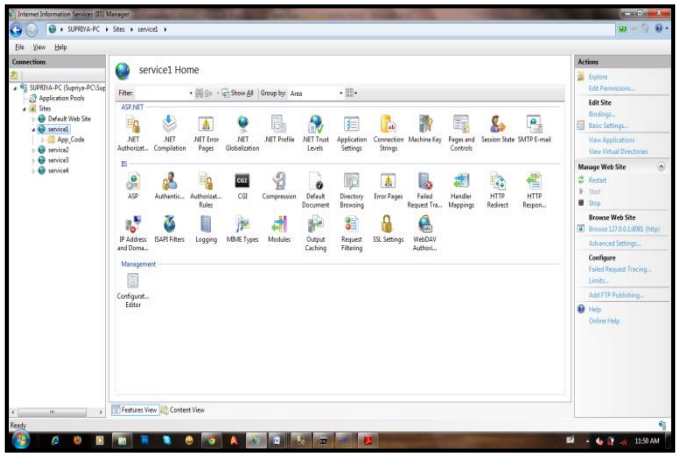
Client need to enter the account number and password. After entering the account number and password it will check the given details with database. If it is same then the user can go to their account.

Beneficiary Types for Transaction



When you need to transfer the fund means first choose the transaction type. Two transaction types will be there. Either we can select transaction within same bank or transaction with other bank.

Web Services



In this we are using three web services other than the main web service viz., web service1, web service2, web service3. If any error or attacks is occurring to the main service the connection will switch to the web service1 and so on.

VI. CONCLUSION

In this system, we addressed the problem of Trustworthy Coordination of Web services atomic transaction for net banking. We have used a suite of protocol for security and reliability of transaction. The main idea we have introduced here is by using the 3PC protocol it is able to reduce the site failures. In 2PC protocol with using AES algorithm if any error occurring then, it will go back to the first phase (Prepared) and will do the Web service searching from beginning. But in 3PC, even though any error occurring it won't go back. Instead, by using Byzantine Agreement Algorithm it will start searching for active Web service. So, it will reduce the searching time.

REFERENCES

[1] M. Steiner, G. Tsudik & M. Waidner (1996), "Diffie-Hellman Key Distribution Extended to Group communication", *Proceedings of 3rd ACM Conference Computer and Communications Security*, Pp. 31-37.

[2] M. Castro & B. Liskov (1999), "Practical Byzantine Fault Tolerance", *Proceedings of the Third Symposium on Operating Systems Design and Implementation*, Pp. 173-186.

[3] M. Gudgin, M. Hadley, N. Mendelsohn, J.J. Moreau, H.F. Nielsen, A. Karmarkar and Y. Lafon (2007), "SOAP Version 1.2 Part 1: Messaging Framework (Second Edition)", *W3C Recommendation*, http://www.w3.org/TR/2007/REC-soap12-part1-20070427/

[4] W. Zhao (2007), "A Byzantine Fault Tolerant Distributed Commit Protocol", *Proceedings of 3rd IEEE International Symposium on Dependable, Autonomic and Secure Computing*, Pp. 37-44.

[5] W. Zhao (2007A), "Byzantine Fault Tolerant Coordination for Web Services Atomic Transactions", *Proceedings of Fifth International Conference on Service-Oriented Computing*, Pp. 307-318.

[6] S.L. Pallemulle, H.D. Thorvaldsson & K.J. Goldman (2008), "Byzantine Fault-Tolerant Web Services for N-Tier and Service Oriented Architectures", *Proceedings of 28th International Conference on Distributed Computing Systems*, Pp. 260-268.

[7] Honglei Zhang, Hua Chai, Wenbing Zhao, Melliar-Smith & Moser (2012), "Trustworthy Coordination of Web Services Atomic Transactions", *IEEE Transactions on Parallel and Distributed Systems*, Vol. 23, No. 8, Pp. 1551-1565.

[8] http://en.wikipedia.org/wiki/Web_service

[9] http://www.investopedia.com/terms/m/message-authentication-code.asp

[10] http://en.wikipedia.org/wiki/Three-phase_commit_protocol

[11] http://en.wikipedia.org/wiki/One-time_password

[12] http://en.wikipedia.org/wiki/Quantum_Byzantine_agreement

Supriya Kurian received B.C.A. degree from Mahatma University, Kerala in 2009. Currently, doing final year M.C.A. in Sathyabama University, Chennai. Research interest includes Web services. Attended workshop on Recent Research Issues on customization of Web Services.

Ramya. G. Franklin completed MCA in Madras University in the year 2004 and finished M.E in Computer Science in the year 2010. Total of 8 years of experience. Currently working as Assistant Professor in the Department of MCA in Sathyabama University. Research interest includes Web services.